G-SETS AND LINEAR RECURRENCES MODULO PRIMES

THOMAS MCKENZIE, SHANNON OVERBAY, AND ROBERT RAY

Abstract. Let p be a prime number with $p \neq 2$. We consider second order linear recurrence relations of the form $S_n = aS_{n-1} + bS_{n-2}$ over the finite field Z_p (we assume $b \neq 0$). Results regarding the period and distribution of elements in the sequence $\{S_0, S_1, \ldots\}$ are well-known (see for example [2, 3, 4, 5]). We examine these second order recurrences using matrices, groups, and G-sets.

1. Introduction

Let $p > 2$ be a prime number and let $S_n = aS_{n-1} + bS_{n-2}$ be a second order linear recurrence with $a, b \in Z_p$ and $b \neq 0$. Since $Z_p \oplus Z_p$ has a finite number of elements, it is clear that any such second order linear recurrence with initial conditions $S_0, S_1 \in Z_p$ will eventually repeat itself. The sequence is called uniformly distributed if each element of Z_p appears the same number of times within a repeated period of the sequence.

The case where $a = b = 1$ is the general Fibonacci sequence whose period was first studied by Wall [4]. The distribution properties of the Fibonacci sequence were explored by Kuipers and Shiue [2]. Webb and Long [5] studied both the period and distribution properties of general second order linear recurrences, providing a complete characterization of such sequences over Z_{p^k}. Niederreiter and Shiue [3] extend the distribution results to finite fields. We examine these second order recurrences over Z_p using matrices, groups, and G-sets.

The sequences defined by the recurrence relation $S_n = aS_{n-1} + bS_{n-2}$ can be generated by the matrix relation

$$\begin{bmatrix} S_{n-1} \\ S_n \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix} \begin{bmatrix} S_{n-2} \\ S_{n-1} \end{bmatrix}.$$

Or equivalently,

$$\begin{bmatrix} S_n \\ S_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^n \begin{bmatrix} S_0 \\ S_1 \end{bmatrix}.$$

Let $A = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}$. Since $b \neq 0$, A is a unit in the ring of 2×2 matrices over Z_p (i.e. $A \in GL_2(Z_p)$). Further, since the group of invertible 2×2 matrices is finite, A generates a finite cyclic group of order m, for some natural number m. We will denote this group by

$$G = \left\{ A^i \mid 0 \leq i \ \leq m-1 \right\}.$$

Left multiplication of matrices on vectors defines a map from $G \times (Z_p \oplus Z_p)$ to $Z_p \oplus Z_p$. Since $A^j \left(A^i v\right) = (A^j A^i)v$, $Z_p \oplus Z_p$ is a G-set (see page 176 of [1]). If a subset U of $Z_p \oplus Z_p$ is closed under this action of G and has the property that for all $u', u \in U$ there exists a $g \in G$ such that $gu = u'$, then we call U a transitive G-set. In other words, the transitive G-sets are just the orbits of the elements of $Z_p \oplus Z_p$ under repeated left multiplication by A.

2. Transitive G-sets

If we select an arbitrary element v from $Z_p \oplus Z_p$, the orbit of v under the action of G is the transitive G-set containing v. These transitive G-sets partition $Z_p \oplus Z_p$.

Example 2.1. *Consider the standard Fibonacci sequence defined by $S_n = S_{n-1} + S_{n-2}$, taken over Z_5. The action of the group generated by $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ partitions the G-set $Z_5 \oplus Z_5$ into the following 3 transitive G-sets (orbits):*

$$H_1 = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\},$$

$$\begin{aligned} H_2 = \Bigg\{ & \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix}, \\ & \begin{bmatrix} 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \Bigg\}, \end{aligned}$$

$$H_3 = \left\{ \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right\}.$$

Example 2.2. *Consider the sequence defined by $S_n = 3S_{n-1} + 4S_{n-2}$, taken over Z_5. Under the action of the group generated by $A = \begin{bmatrix} 0 & 1 \\ 4 & 3 \end{bmatrix}$, the G-set $Z_5 \oplus Z_5$ can be partitioned into the following 5 transitive G-sets (orbits):*

$$G_1 = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\},$$

$$G_2 = \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix} \right\},$$

$$G_3 = \left\{ \begin{bmatrix} 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \end{bmatrix} \right\},$$

$$G_4 = \left\{ \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \end{bmatrix} \right\},$$

$$G_5 = \left\{ \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \end{bmatrix} \right\}.$$

To further study the structure of the transitive G-sets, we turn to the eigenvalues and eigenvectors associated with the matrix A. If $\lambda \in Z_p$ is a root of the characteristic polynomial $C(x) = x^2 - ax - b$, then we will denote the associated eigenspace by E_λ. The dimension of E_λ must be one or two. We note that by its construction, $A \neq \lambda I$, so E_λ must be one dimensional. It can be verified that $\begin{bmatrix} 1 \\ \lambda \end{bmatrix}$ is an eigenvector in E_λ. Thus,

$$E_\lambda = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ \lambda \end{bmatrix}, \begin{bmatrix} 2 \\ 2\lambda \end{bmatrix}, \begin{bmatrix} 3 \\ 3\lambda \end{bmatrix}, \dots, \begin{bmatrix} p-1 \\ (p-1)\lambda \end{bmatrix} \right\}.$$

It is easy to check that $\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$ will always be a transitive G-set under the action of G on $Z_p \oplus Z_p$. It is also easy to see that if a transitive G-set contains an eigenvector, all the other vectors in that transitive G-set must also be eigenvectors. Therefore, for any transitive G-set, there are three mutually exclusive possibilities:

(1) it is the transitive G-set $\left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$,
(2) it consists entirely of eigenvectors,
(3) it consists entirely of nonzero noneigenvectors.

In Example 2.2, the characteristic polynomial $C(x)$ has repeated root $\lambda = 4$ with associated eigenspace

$$E_4 = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \end{bmatrix} \right\}.$$

In this example, G_4 and G_5 are comprised only of eigenvectors, G_2 and G_3 are comprised only of nonzero noneigenvectors, and G_1 is of course, just

$\left\{\begin{bmatrix}0\\0\end{bmatrix}\right\}$. Additionally, if we let $S_0 = 0$ and $S_1 = 1$, the sequence generated by $S_n = 3S_{n-1} + 4S_{n-2}$ is

$$0, 1, 3, 3, 1, 0, 4, 2, 2, 4, 0, 1, 3, 3, \ldots$$

which repeats after the tenth term and corresponds to the elements of the transitive G-set G_2. If we choose different starting conditions, e.g. $S_0 = 0$ and $S_1 = 4$, we get a similar, shifted sequence that also corresponds to G_2.

In Example 2.1, the characteristic polynomial $C(x)$ has a repeated root $\lambda = 3$, with corresponding eigenspace

$$E_3 = \left\{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\3\end{bmatrix}, \begin{bmatrix}2\\1\end{bmatrix}, \begin{bmatrix}3\\4\end{bmatrix}, \begin{bmatrix}4\\2\end{bmatrix}\right\}.$$

We note that the transitive G-set H_3 contains only eigenvectors and H_2 consists entirely of nonzero noneigenvectors. Furthermore, every set of initial conditions outside the eigenspace E_3 lies within the single transitive G-set H_2. Choosing the initial starting values $S_0 = 0$ and $S_1 = 1$, the Fibonacci sequence over Z_5, generated by $S_n = S_{n-1} + S_{n-2}$, is

$$0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, \ldots.$$

This sequence repeats after 20 terms and corresponds to the elements of the transitive G-set H_2. If, instead, we take the initial starting values of $S_0 = 2$ and $S_1 = 1$, we will generate the Lucas numbers over Z_5. The corresponding sequence is

$$2, 1, 3, 4, 2, 1, 3, 4, \ldots.$$

In this case, the initial conditions correspond to the eigenvector $\begin{bmatrix}2\\1\end{bmatrix}$, so the sequence corresponds to H_3. We note that in the Fibonacci sequence over Z_5, each element of Z_5 appears the same number of times before the sequence repeats, while the element 0 does not appear in the sequence of Lucas numbers over Z_5. The distribution properties of these sequences will be discussed in greater detail in the next section.

3. Distribution of Elements

In Example 2.2, the initial starting conditions $S_0 = 0$ and $S_1 = 1$ produce the uniformly distributed repeated sequence $0, 1, 3, 3, 1, 0, 4, 2, 2, 4$; whereas the initial conditions $S_0 = 1$ and $S_1 = 4$ result in the nonuniformly distributed repeated sequence $1, 4$.

As we noted above, each element of the eigenspace associated with λ is a multiple of $\begin{bmatrix}1\\\lambda\end{bmatrix}$, so the vector $\begin{bmatrix}0\\0\end{bmatrix}$ will be the only vector within an eigenspace that contains a zero entry. But, we know that $\begin{bmatrix}0\\0\end{bmatrix}$ lies within its own transitive G-set. Thus, the sequences generated by initial conditions $\begin{bmatrix}S_0\\S_1\end{bmatrix}$ taken from an eigenspace will not be uniformly distributed. Hence, we will focus our attention on the transitive G-sets comprised of nonzero noneigenvectors. We first show that each of these transitive G-sets have equal size.

Theorem 3.1. *If the order of A is m and $v \in Z_p \oplus Z_p - \left\{\begin{bmatrix}0\\0\end{bmatrix}\right\}$ is not an eigenvector of A, then the transitive G-set generated by v has exactly m elements.*

Proof. Let $n \in \{1, \ldots, m\}$ with $A^n(v) = v$. Applying A to both sides of the last equality yields $A^n(A(v)) = A(v)$. Since v is a noneigenvector, v and $A(v)$ are linearly independent, forming a basis for $Z_p \oplus Z_p$. But, A^n fixes both v and $A(v)$, thus A^n is the identity, so $n = m$. This gives the result. $\square$

The characteristic polynomial $C(x)$ of A, has one repeated root, two distinct roots, or no roots in Z_p. Then the discriminant of $C(x)$ is $a^2 + 4b$. We noted above that if λ is a root of $C(x)$ then E_λ has exactly p elements. We make the following observations.

1. If A has exactly one eigenvalue in Z_p, then A has exactly $p^2 - p$ nonzero noneigenvectors. This corresponds to the case where $a^2 + 4b = 0$.
2. If A has exactly two eigenvalues in Z_p, then A has exactly p^2-2p+1 nonzero noneigenvectors. This corresponds to the case where a^2+4b is a nonzero square (quadratic residue) in Z_p.
3. If A has no eigenvalues in Z_p, then A has exactly $p^2 - 1$ nonzero noneigenvectors. This corresponds to the case where $a^2 + 4b$ is not a square in Z_p.

Now the following corollary is clear.

Corollary 3.2.

(i) *If A has exactly one eigenvalue in Z_p, then the number of elements in any transitive G-set of nonzero noneigenvectors divides $p^2 - p$.*

(ii) *If A has exactly two eigenvalues in Z_p, then the number of elements in any transitive G-set of nonzero noneigenvectors divides p^2-2p+1.*

(iii) *If A has no eigenvalues in Z_p, then the number of elements in any transitive G-set of nonzero noneigenvectors divides $p^2 - 1$.*

Proof. This follows immediately from the last theorem and the above observation. □

Corollary 3.3. *If A does not have exactly one eigenvalue in Z_p and if v is a nonzero noneigenvector of A, then the sequence generated by the initial conditions* $\begin{bmatrix} S_0 \\ S_1 \end{bmatrix} = v$ *is not uniformly distributed.*

Proof. Z_p has p elements, but by parts (ii) and (iii) of the last Corollary, p cannot divide the number of elements in this sequence. □

4. Uniform Distribution

Now we focus our attention on the case where the characteristic polynomial has a repeated eigenvalue λ. Let r be the order of λ in the multiplicative group Z_p^*.

Theorem 4.1. *If the second order recurrence $S_n = aS_{n-1} + bS_{n-2}$ has characteristic polynomial $C(x) = x^2 - ax - b$ with a repeated root λ and the initial conditions are $S_0 = 0$ and $S_1 = t$, then the general term of the sequence is given by $S_n = tn\lambda^{n-1}$.*

Proof. It is well-known that the general solution to this type of second order recurrence with a repeated root has the form $S_n = (\alpha + \beta n)(\lambda^n)$. Using the initial conditions $S_0 = 0$ and $S_1 = t$, we have: $0 = S_0 = \alpha$ and $t = S_1 = \beta\lambda$, which gives us $\alpha = 0$ and $\beta = t\lambda^{-1}$. Plugging these values in for α and β gives us the desired result. □

The form, $S_n = tn\lambda^{n-1}$, gives us some useful information. First, we recall that the $p-1$ nonzero elements of Z_p form the multiplicative group Z_p^*. Since $\lambda \neq 0$, by Lagrange's Theorem, r must divide $p-1$. In particular, $\lambda^{p-1} = 1$ and $\lambda^p = \lambda$. Also, since Z_p has characteristic p, it follows that every pth term of $S_n = tn\lambda^{n-1}$ will be 0. Furthermore, if $t \neq 0$, we see that the terms $S_1, S_2, \ldots, S_{p-1}$ are not zero. The term $S_p = tp\lambda^{p-1} = 0$ and the term $S_{p+1} = t(p+1)\lambda^p = t\lambda$, which gives us our initial conditions, multiplied by λ. This means that the next p terms of the sequence will be the same as the first p terms multiplied by λ. Similarly, $S_{2p} = 0$ and $S_{2p+1} = t(2p+1)\lambda^{2p} = t\lambda^2$. So, again, the next p terms are attained by multiplying the previous p terms by λ. This will continue until we reach the order of λ. Since $\lambda^r = 1$, $S_{rp} = 0$ and $S_{rp+1} = t(rp+1)\lambda^{rp} = t\lambda^r = t$, so we return to the initial starting conditions. Thus, the period of the sequence must divide rp. Since $t \neq 0$, and $\lambda, \lambda^2, \ldots, \lambda^{r-1}$ are distinct, then the first time the initial conditions are repeated is when $n = rp$, thus the period is equal to rp.

We also note that each of the rp pairs of consecutive elements S_{n-1}, S_n, where $n = 1, 2, \ldots, rp$ are distinct since

$$\begin{bmatrix} S_n \\ S_{n+1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^n \begin{bmatrix} 0 \\ t \end{bmatrix}.$$

If we had repeated elements, then

$$\begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^{n_1} \begin{bmatrix} 0 \\ t \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^{n_2} \begin{bmatrix} 0 \\ t \end{bmatrix}$$

for some integers n_1 and n_2 with $0 < n_1 < n_2 < rp$. Since the matrix is invertible, this would give us:

$$\begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}^{n_2 - n_1} \begin{bmatrix} 0 \\ t \end{bmatrix} = \begin{bmatrix} 0 \\ t \end{bmatrix},$$

which would mean we would repeat the initial conditions before rp, so the period would be smaller than rp. Thus, the list of rp vectors in the corresponding transitive G-set, starting with $\begin{bmatrix} 0 \\ t \end{bmatrix}$ will all be distinct. Now we can generate the remaining transitive G-sets by starting with a vector of the form $\begin{bmatrix} 0 \\ s \end{bmatrix}$, where $s \neq 0$, that does not appear in the first transitive G-set. This transitive G-set will also have size rp. Continue until all $p(p-1)$ of the nonzero noneigenvectors are accounted for.

Now we have the following theorem.

Theorem 4.2. *If the second order recurrence $S_n = aS_{n-1} + bS_{n-2}$ has characteristic polynomial $C(x) = x^2 - ax - b$ with a repeated root λ of order r, then every transitive G-set associated with a vector outside the eigenspace has size rp.*

Theorem 4.3. *Let λ be a repeated root of the characteristic polynomial $C(x) = x^2 - ax - b$ associated with $A = \begin{bmatrix} 0 & 1 \\ b & a \end{bmatrix}$. If E_λ is the eigenspace generated by $\begin{bmatrix} 1 \\ \lambda \end{bmatrix}$, then each coset of the form $\begin{bmatrix} 0 \\ t \end{bmatrix} + E_\lambda$, where $t = 1, 2, \ldots, p-1$, will lie within a single transitive G-set.*

Proof. We will show that the subgroup of G generated by A^r acts transitively on each of these cosets. Hence, each coset will reside in a single transitive G-set induced by left multiplication by A. We first note that the characteristic polynomial of A can be written as $x^2 - ax - b$ or as $x^2 - 2\lambda x + \lambda^2$. As such, $a = 2\lambda$ and $b = -\lambda^2$, so the matrix A can also be written as $\begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix}$. It is easily shown by induction that

$$A^n = \begin{bmatrix} 0 & 1 \\ -\lambda^2 & 2\lambda \end{bmatrix}^n = \begin{bmatrix} (1-n)\lambda^n & n\lambda^{n-1} \\ -n\lambda^{n+1} & (n+1)\lambda^n \end{bmatrix}.$$

If v is any vector in $Z_p \oplus Z_p$, we can show that $A^r v - v$ is in E_λ by showing that it is in the null space of $A - \lambda I$. By direct calculation it is easily verified that

$$[A - \lambda I]\,[A^r - I]v = 0$$

since

$$\begin{bmatrix} -\lambda & 1 \\ -\lambda^2 & \lambda \end{bmatrix} \begin{bmatrix} (1-r)\lambda^r - 1 & r\lambda^{r-1} \\ -r\lambda^{r+1} & (r+1)\lambda^r - 1 \end{bmatrix} v = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} v.$$

Since $A^r v$ and v differ by an eigenvector, they are in the same coset. In particular, if $v = \begin{bmatrix} 0 \\ t \end{bmatrix}$, where $t \neq 0$, v is not an eigenvector, so $A^{kr}v$ are distinct vectors for $0 \leq k \leq p-1$ (see Theorem 4.2). Consequently, we have $\left\{A^{kr}v \mid 0 \leq k \leq p-1\right\} = v + E_\lambda$. □

Since E_λ is generated by $\begin{bmatrix} 1 \\ \lambda \end{bmatrix}$, every element of Z_p appears in the top entry exactly once and in the lower entry exactly once in the vectors of E_λ. In other words, the elements of Z_p are distributed uniformly in the rows of the vectors of E_λ. The cosets formed by adding $\begin{bmatrix} 0 \\ t \end{bmatrix}$ to the vectors in E_λ merely shift the lower entries of E_λ by t, so the distribution of elements of Z_p remains uniform in the rows of the vectors in each of these cosets. Since a particular coset of this form lies entirely within a single transitive G-set, each such transitive G-set is the union of r of these cosets. Hence, the transitive G-sets associated with nonzero noneigenvectors are uniformly distributed. This leads us to the following theorem.

Theorem 4.4. *Let A be the matrix associated with second order recurrence $S_n = aS_{n-1} + bS_{n-2}$. If the characteristic polynomial $C(x) = x^2 - ax - b$ has a repeated root λ then the transitive G-set induced by left multiplication by A will be uniformly distributed if and only if the initial vector $v = \begin{bmatrix} S_0 \\ S_1 \end{bmatrix}$ is not an element of the eigenspace E_λ.*

In Example 2.2, the characteristic polynomial had one repeated root, $\lambda = 4$, of order 2 in Z_5. The associated eigenspace is:

$$E_4 = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \begin{bmatrix} 4 \\ 1 \end{bmatrix} \right\}.$$

Adding the vector $\begin{bmatrix} 0 \\ t \end{bmatrix}$, where $t = 1, 2, 3, 4$, to each element of the eigenspace, we obtain four additional cosets of five vectors:

$$\left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \end{bmatrix}, \begin{bmatrix} 4 \\ 2 \end{bmatrix} \right\};$$
$$\left\{ \begin{bmatrix} 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}, \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \begin{bmatrix} 4 \\ 3 \end{bmatrix} \right\};$$
$$\left\{ \begin{bmatrix} 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 4 \\ 4 \end{bmatrix} \right\};$$
$$\left\{ \begin{bmatrix} 0 \\ 4 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 0 \end{bmatrix} \right\}.$$

The twenty vectors in these four cosets, along with the original eigenspace, cover all of $Z_5 \oplus Z_5$.

Note that G_2 and G_3 are the two transitive G-sets of nonzero noneigenvectors. Each has size $10 = 2(5) = rp$. In this example, each transitive G-set formed with vectors outside the eigenspace consists of two complete cosets and every other element of each such transitive G-set comes from the same coset. Since each coset is uniformly distributed, so is each corresponding transitive G-set. Thus we see that any pair of starting conditions, other than those in the eigenspace, results in a uniformly distributed sequence with period rp.

In Example 2.1, the cosets of the form $\begin{bmatrix} 0 \\ t \end{bmatrix} + E_3$, where $t = 1, 2, 3, 4$, all lie within the transitive G-set H_2. In this case, the repeated eigenvalue $\lambda = 3$ has order $r = 4$. This single set of nonzero noneigenvectors has $20 = 4(5) = rp$ elements. Any pair of initial conditions taken from H_2 will yield a uniformly distributed sequence which repeats after 20 terms, whereas sequences with initial contitions taken from H_1 or H_3 will produce nonuniformly distributed sequences.

5. Acknowledgments

We would like to thank the referee for a careful reading of this paper and valuable suggestions. We would also like to thank Dr. John Burke for introducing us to this problem several years ago. It has led to many interesting new discoveries which we hope to continue to explore.

References

[1] M. Artin, *Algebra*, Prentice Hall, New Jersey, 1991.
[2] L. Kuipers and J. S. Shiue, *A distribution property of the sequence of Fibonacci numbers*, The Fibonacci Quarterly, **10.4** (1972), 375–392.

[3] H. Niederreiter and J. S. Shiue, *Equidistribution of linear recurring sequences in finite fields*, Indag. Math., **80** (1977), 397–405.
[4] D. D. Wall, *Fibonacci series modulo m*, The American Mathematical Monthly, **67** (1960), 525–532.
[5] W. A. Webb and C. T. Long, *Distribution modulo p of the general second order recurrence*, Atti Accad. Lincei, **58** (1975), 92–100.

MSC2010: 11B50

Key words and phrases: matrix groups, linear recurrences over Z_p

Department of Mathematics, Gonzaga University, Spokane, WA
E-mail address: `mckenzie@gonzaga.edu`

Department of Mathematics, Gonzaga University, Spokane, WA
E-mail address: `overbay@gonzaga.edu`

Department of Mathematics, Gonzaga University, Spokane, WA
E-mail address: `rayr@gonzaga.edu`